COPY PROTECTION WITHOUT NON-VOLATILE MEMORY

ABSTRACT

An FPGA includes a plurality of configurable logic elements, a configuration circuit, a decryption circuit, and a fingerprint element. The fingerprint element generates a fingerprint that is indicative of inherent manufacturing process variations unique to the FPGA. The fingerprint is used as a key for an encryption system that protects against illegal use and/or copying of configuration data. In some embodiments, the propagation delay of various circuit elements formed on the FPGA are used to generate the fingerprint. In one embodiment, the specific frequency of an oscillator is used to generate the fingerprint. In some embodiments, a ratio of measurable values may be used to generate the fingerprint. In other embodiments, differences in transistor threshold voltages are used to generate the fingerprint. In still other embodiments, variations in line widths are used to generate the fingerprint.